REMARKS

The present response is intended to be fully responsive to all points of objection and/or rejection raised by the Examiner and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the application is respectfully requested.

Applicants assert that the present invention is new, non-obvious and useful. Prompt consideration and allowance of the claims is respectfully requested.

Status of Claims

Claims 1 through 13 have been canceled.

claims 14 through 28 are on file.

Claims 14, 16, 19, 20, 22, 23 are Currently Amended.

CLAIM REJECTIONS

35 U.S.C. § 103 Rejections

Further to the examiner comment in the office action, the applicant has decided, for clarity reasons, and to avoid all examiner rejections, to amend the claims accordingly and as listed above.

The objective of the amended claims, is to explicitly recite the limitation that the device is associate with its user (i.e. the user is the owner of the device), and that the device issues a certified digital document that is associated with the **user of the device**.

On Pages 2-3 of the Office Action, the Examiner has rejected claims 14-19, 21-24, 26 under 35 U.S.C. §103(b) as being anticipated by Micali, US Patent No. 5,604,804 ("Micali") in view of Muftic, US patent No 5745574, "Muftic".

Micali discloses a method for certifying public keys in a digital signature scheme by an authority. Conversely independent amended claims 14 & 22 clearly recite the limitation of generating a new digital document by the user's device that is associated with its user. In **Micali,** it is clear that the authorities are not associated with the user. Micali does not disclose, teach or suggest this limitation. Further more, it would be obvious to one that have skills in the art, that in embodiment such as Micali describes, the authority can't be associated with the user, because such said authority has to be trusted by the CA. In Micali's embodiment, a user that wished to certify his public key can not be trusted by the CA, as he was not inspected by that CA previously and thus, is not associated with that CA. The limitation of a user's device that is associated with its user is not suggested, taught or disclosed by **Micali**. As well established under U.S. patent law, for a reference to anticipate a claim, the reference must teach all elements of the claim.

Further more, and as was already explained in our previous response to the previous office action, the examiner alleges that Micali "**discloses the implementing in device a document issuing policy of the CA see Col 2 Ln 17-31** ;". Applicants still fails to see how the cited paragraph is relevant to the implementing in device a document issuing method of a certifying authority (CA). Further more, new amended claims 14 & 22 clearly cite the limitations that a document issuing policy is implemented into a device, and that the documents that are generated, are on behalf of **that same CA**. For example, the cited paragraph disclose the need of accountability of intermediate authorities "**if a user presents an intermediate authority with a piece of data to be certified, such as public key, and the intermediate authority individually certifies the data and passes this certification on to a higher authority who issues the certificate, the intermediate authority should not be able to latter deny having contributed to the certification of the piece of data**". Nowhere

in the referred paragraph the limitation of ***implementing in device a document issuing policy of the CA*** is disclosed, taught or suggested.

The examiner had also alleged that Micali discloses "***reading into device a certified document associated with user see Col 3 Ln 13 – 28***". Applicants still fail to see how the cited paragraph is relevant to the reading into device a certified document associated with user. According to Micali in the cited paragraph : "***The piece of data that is presented may be a public key having at least one corresponding secret key. A user may choose the public key to be used in connection with either a digital signature system or a public key encryption system***". Therefore, it is clear that the user chooses the piece of data to be certified. Independent new amended claims 14 & 22 clearly recite the limitation that the read document has to be a certified document. In distinction to Micali, in the present invention a certified document (that already has been issued by a CA) is to be read into the device. Nowhere in the referred paragraph this limitation is disclosed, taught or suggested. As well established under U.S. patent law, for a reference to anticipate a claim, the reference must teach all elements of the claim.

The examiner also alleges that Micali, in view of Muftic, discloses "***generating on behalf of CA a new certified document based on read document see Col 6 Ln 14-26***". Applicant fails to see how Muftic is relevant to the cited patent of Micali. The essence of Micali's patent is to enable issuing authorities to add information to its own generated certificates in order to leave accountability. Furthermore, nowhere in the cited paragraph, the clear limitation that the CA, which is associated with the implemented document issuing policy, and the CA which the device acts on behalf of it(CA), is the same CA, is disclosed taught or suggested. The cited paragraph is not relevant to generating on behalf of the CA a new certified digital document based on the read certified digital document and issuing policy (of the same CA). For example it is disclosed in the cited paragraph that the issuing authority can add information to its own issuing certificate to prove the accountability of intermediate authorities that contributed to the certification: "***The issuing authority may cause additional information to be saved which, when combined with the information that is stored, proves that the intermediate authorities contributed to certification of the piece of data.***" And so

on. It would be illogical to examine Micali in view of Muftic, as if the issuing authority issues the certificate as the parent CA it would not have to cause additional information to be saved to prove the intermediate authorities accountability. Nowhere in the referred paragraph, a device generating on behalf of a CA a new certificate associated with the user of the device, based on a read certified document and an issuing policy previously implemented in the device (by the same CA), is disclosed taught or suggested. As well established under U.S. patent law, for a reference to anticipate a claim, the reference must teach all elements of the claim.

Regarding examiner rejection of claim 15, Examiner alleges that Micali "***discloses the identity of device in form of digital signature stored with intermediate CA see Col 4 Ln 18-42.***" Claim 15 clearly cites the limitation that the identity "is stored within the electronic device". Applicants fail to see how the cited paragraph is relevant for storing the identity of the device or its user within the electronic device. For example the cited paragraph discloses that additional identifying information of an intermediate authority can be saved and added to the signature of another authority in order to prove that the intermediate authority contributed to the certificate to be issued: "***The portion of the digital signature may be combined to prove that it contributed to the certificate being issued***". Nowhere in the referred paragraph, information associated with the identity of the electronic device itself or its user is disclosed, taught or suggested. As well established under U.S. patent law, for a reference to anticipate a claim, the reference must teach all elements of the claim.

Regarding examiner rejection of claims 16, 24 Examiner alleges that Micali "***discloses the policy attests to personal identifying information of user*** **see Col 6 Ln 28-39**". Applicants fail to see how the cited paragraph is relevant to the issuing policy **attesting** personal identifying information of the user. Claims 16, 24 clearly recite that issuing policy attest personal identiftying information of the user. Micali does not disclose, teach or suggest that an issuing policy attests the user of the device. Conversely for example, in the cited Paragraph Micali disclose that information that is stored can be stored in a way to prove in the future the identity of a witness: "***The portion of the digital signature can be combined to***

prove that the intermediate authorities contributed to certification of the piece of data". Nowhere in the referred paragraph a certificate issuing policy that attests to the device's user personal identifying information is disclosed, taught or suggested. As well established under U.S. patent law, for a reference to anticipate a claim, the reference must teach all elements of the claim.

Regarding claim 17, Examiner alleges that Micali "***discloses the certified document being output thorough a secure channel see Col 5 Ln 20-36***". In the cited paragraph Micali discloses the need to limit or save certificate size in a communication systems "***Such transmission and storage costs, however, are incurred...".*** Applicants Claim 17 is dependent on Claim 14, and allows the method of Claim 14 to be output through a communication channel. Therefore this claim 17 should be allowed in conjunction with Claim 14.

Regarding claim 18, Examiner alleges that Micali "***discloses the digital documents being certificates and permits see Col 5 Ln-37-45***" Applicants read carefully the cited paragraph of Micali and failed to see any disclosure, teaching or suggestion by Micali that documents might or could be permits. Furthermore, Claim 18 is dependent on Claim 14, and allows the method of Claim 14 to be output as a permit or certificate. Therefore this claim 18 should be allowed in conjunction with Claim 14

Regarding claims 19 and 21, 26 , Examiner alleges that Micali "***discloses the signing of certificates and authorities along the path see Col 6 Ln 14-26***". Applicants fail to see the relevance of the cited paragraph to Claim 19, and 21, 26. For example, in the cited Paragraph Micali discloses that certificate issuing authorities can include additional information to their issued certificates: "***The issuing authority may cause additional information to be saved which, when combined with the information that is stored, proves that the intermediate authorities contributed to certification of the piece of data.***" . In distinct to Micali, Claim 19 of the present invention claims that identification of a user by the device is being performed prior to the action of the device to sign or certify a digital document. Furthermore, Claims 21

and 26 of the present invention claim that a "***plurality of certified digital documents associated with the user is stored within the electronic device...each of which is associated with a different certifying authority***". Nowhere in the cited paragraph the identification of a user to the device prior to the device signs or certifies a digital document, nor the storing of a plurality of certified digital document in a device is disclosed, taught or suggested.

For clarity, we cite again from our last response to the office action, explaining the great difference between Micali and our patent application.

According to Micali "***According to the present invention, certifying pieces of data in a system with at least two levels of authorities includes presenting a piece of data requiring certification to a first level authority causing a higher authority to receive an indication ..... having the higher authority issue a certificate that the piece of data possesses the given property.... And storing information in order to keep at least the first level authority accountable...***" (Col. 2 Line 57 – Col. 3 Line 3). It is clear that Micali discloses a mechanism that involves at least two levels of authorities, to store information in a certificate and to keep an intermediate level authority accountable for the issuing of the certificate by a higher authority, rather than implementing in device a document issuing policy of the CA, as disclosed in the present invention.

In distinction to Micali, the present invention discloses a method to authorize an electronic device ("smart card") to act as a representative of the CA itself, without the need of an intermediate authority ("***This method, in fact, transform the smart card into a subcontractor of that known Certifying Authority (CA), for the purpose of issuing permits or certificates. Thus, the smart card now can issue permits or certificates on behalf of the original CA authority.***", Page 3, pars. 84-85.).

Making a smart card a representative of a CA eliminates the need for making intermediate authorities accountable for signing or certifying, because the smart card acts as the CA itself (***",..., the device will operate as a certified authority according to the***

program or document issuing method that originates with the known authority", Page 9 par. 279). This means that the (genuine) CA is replaced (represented) by the smart card.

In view of the foregoing remarks, the pending claims are deemed to be allowable. Their favorable reconsideration and allowance is respectfully requested.

Respectfully submitted,

E. Barkan

Elad Barkan
12 Habanin Street,
Kefar Sirkin 49935,
ISRAEL
Email: moti@barkan.org